

Europäisches Patentamt
European Patent Office
Office européen des brevets



(11)

EP 0 786 881 A2

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
30.07.1997 Bulletin 1997/31

(51) Int. Cl.⁶: H04L 9/12

(21) Application number: 96309516.1

(22) Date of filing: 27.12.1996

(84) Designated Contracting States:
DE FR GB

(30) Priority: 29.01.1996 US 592931
29.01.1996 US 592903

(71) Applicant: INTERNATIONAL BUSINESS
MACHINES CORPORATION
Armonk, NY 10504 (US)

(72) Inventors:
• Gray, James P.
Chapel Hill, NC 27514 (US)

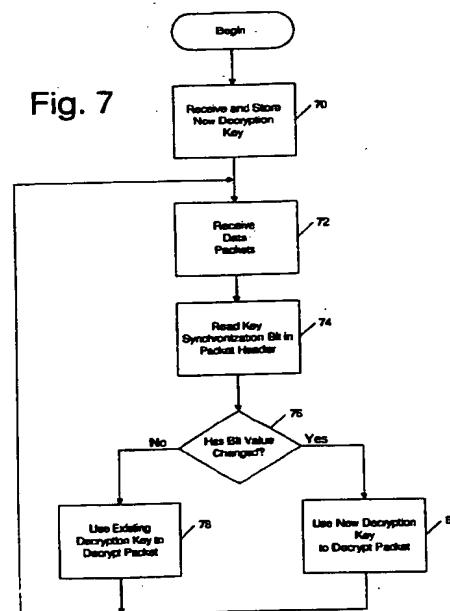
• Onvural, Ralf O.
Cary, NC 27513 (US)
• Peyravian, Mohammed
Cary, NC 27513 (US)

(74) Representative: Moss, Robert Douglas et al
IBM United Kingdom Limited
Intellectual Property Department
Hursley Park
Winchester Hampshire SO21 2JN (GB)

(54) **Method and system for synchronisation of encryption/decryption keys in a data communications network using marker packets**

(57) To enhance the security provided by data encryption in a data communication network, encryption/decryption keys are changed periodically at the source and destination nodes for an established connection. A destination node must know not only the value of any new key but also when to begin using that key to decrypt received data packets. Synchronization (making sure a data packet is decrypted using a decryption key correlated with the encryption key used to encrypt the same packet) is achieved through the use of marker cells, special purpose cells. When a source node decides to activate a new key, previously sent to and stored at the destination node, a marker cell is transmitted by the source node to the destination node. When the destination node recognizes the marker packet, it discards it and activates the previously received key for use in decrypting subsequently received packets.

Fig. 7



EP 0 786 881 A2

Description

Field of the Invention

The present invention relates to data communications and more particularly to a technique for using marker packets to synchronize the use of encryption and decryption keys at source and destination nodes in a data communication network..

Background of the Invention

Data communication networks can be categorized as handling transfers of data on either a circuit-switched basis or a packet-switched basis. Where two users want to exchange data in a network which utilizes circuit switching, a path must be established through the network before the data exchange can begin. Once the path is set up, it continues to exist for the duration of the data exchange between the users. If the same two users were connected through a packet-switched network, it would not be necessary to set up and maintain a "circuit" between them. In a packet-switched network, user data is formatted in discrete data units or packets, each of which contains the routing information needed by intermediate systems or nodes to transfer the packet toward its intended destination over currently available links. When an information exchange or call has been set up between a particular source node and a particular destination node, it is conventionally said that a "connection" exists between the two nodes even though there is no physical connection and successive data packets being transferred between the nodes may not even follow the same physical paths through the network in getting from the source node to the destination node.

A type of packet-switching technology that is becoming increasingly pervasive is Asynchronous Transfer Mode (ATM) technology. In ATM networks, user data is formatted in fixed length cells, each of which includes a header field and a data field. The standard header field is five bytes in length and contains all necessary control and routing information for allowing the cell to be switched through the network toward its destination. The standard data field is forty-eight bytes long. The use of fixed length cells permits much of the necessary switching within the network to be carried out using specialized, high-speed hardware switches.

Users of any kind of data communication network, and not just ATM networks, are often concerned about concealing their data from eavesdroppers (sometimes called interlopers) on the network. Considerable time and effort has been spent developing cryptographic techniques which permit original data (sometimes referred to as plaintext or cleartext) to be encrypted or "scrambled" before it is transmitted as "ciphertext" through the network and then decrypted or returned to its original or plaintext form once it reaches the intended destination. Many encryption techniques employ "keys",

which are values that control the encryption and decryption processes.

An illustration of an extremely simple, and largely ineffective, encryption approach is to replace each plaintext character in a message by a character "n" positions away in the alphabet, wrapping or returning to the beginning of the alphabet where the plaintext character is within "n" positions of the end of the alphabet. For example, if $n = 3$, the plaintext word "safe" would translate to the ciphertext word "vdih". In this example, 3 would be considered the encryption key. As long as the party receiving the ciphertext message knows the encryption method and the key, recovery of the plaintext message is relatively simple.

Any effort by an eavesdropper to recover plaintext from an encrypted message is referred to as an "attack" on the message. Just as there are different kinds of encryption, there are different kinds of attacks aimed at discovering the key used to encrypt the plaintext data. Where a user must select the encryption key, it is human nature for that user to select an easily remembered key, such the user's own last name or the name of a favourite hobby; e.g., "golf" or "sailing". Eavesdroppers can take advantage of human nature by employing a "dictionary attack" in which names, English words (for example, all of the words in an unabridged dictionary), birthdays, etc. are tried as decryption keys to see if plaintext is generated. Where an eavesdropper knows the names of the sending and/or receiving parties or the time of transmission of the ciphertext message or other transmission-related information, a "traffic analysis attack" may be mounted by using such information in an effort to find the encryption key. More detailed information about the subject of cryptography is available from a number of references, including the book Bruce Schneier, "Applied Cryptography - Protocols, Algorithms and Source Code in C", John Wiley & Sons (1994). While the present invention is intended for use in networks in which cryptography is practised, the invention can be understood without requiring any information from this book.

In theory, nothing precludes the performance of encryption/decryption operations without changing the keys used to control such operations. In practice, it would be foolish to do that. The longer a particular key remains in use, the greater the chance that an interloper will discover that key and use it in a successful attacks on encrypted messages.

A standard data security practice is to periodically change the keys used for encryption/decryption operations. Each new key must be passed on to any node expected to decrypt data encrypted using that key. Equally significantly, a decrypting node must know when to begin using a new key. If a destination node uses an old key in an attempt to decrypt data encrypted at a source node using a new key, the destination node's output will be plaintext garbage, not useful data.

Conventionally, encryption/decryption keys are established when a connection is set up between two

nodes and remain in use for the duration of the connection. Since some connections may persist for periods of weeks or even months, for example, between two host systems, a failure to change the keys other than at connection setup represents a data security risk.

Summary of the Invention

According to one aspect, the present invention provides, for use in a system including one or more source nodes for encrypting data using an encryption key, an interposed data communication network through which packets including the encrypted data can be transmitted, each of said packets including a header and a data payload, and one or more destination nodes capable of decrypting received data using a decryption key, a method of maintaining synchronization between the encryption key used at a source node to encrypt data and the decryption key used at the destination node to decrypt data, said method comprising the steps of: sending a new decryption key from the source node to the destination node, storing the new decryption key at the destination node, at the source node, transmitting a data packet having a predetermined format when the new decryption key is to be activated; at the destination node, monitoring each received data packet to determine whether the packet has the predetermined format; and at the destination node, when a packet having the predetermined format is detected, activating the new decryption key for use in decrypting subsequently received packets.

According to another aspect, the present invention provides, for use in a system including one or more source nodes for encrypting data using an encryption key, an interposed data communication network through which data packets including the encrypted data can be transmitted, each of said data packets including a header portion and a data payload portion, and one or more destination nodes for decrypting received data packets using a decryption key, a key-synchronizing system for maintaining synchronization between the encryption key used at a source node to encrypt data and the decryption key used at the destination node to decrypt data, said key-synchronizing system comprising: at a source node from which the encrypted packet is to be sent, means for sending at least one new decryption key to the destination node which is to receive the packet; at the destination node, means storing each new decryption key that is received; at the source node, means for generating a data packet having a predetermined format; at the destination node, means for monitoring each received data packet and for determining whether the packet has the predetermined format; and at the destination node, means responsive to the identification of a received data packet having the predetermined format for retrieving a new decryption key from storage and for initiating use of that key to decrypt each subsequently received data packet.

According to another aspect, the present invention

provides a key-synchronizing source node for use in a system including one or more source nodes for encrypting data using an encryption key, an interposed data communication network through which data packets including the encrypted data are transmitted, each of said data packets including a header portion and a data payload portion, and one or more destination nodes for decrypting received data packets using a decryption key, said key-synchronizing source node comprising: means for sending at least one new decryption key to a destination node to which data packets are to be sent; means for generating a data packet having a predetermined format, indicating that a new decryption key is to be activated at a destination node to which the data packet having the predetermined format is sent; and means for sending the data packet having the predetermined format to at least one destination node.

According to another aspect, the present invention provides a key-synchronizing destination node for use in a system including one or more source nodes for encrypting data using an encryption key, an interposed data communication network through which data packets including the encrypted data is transmitted, each of said data packets including a header portion and a data payload portion, and one or more destination nodes for decrypting received data packets using a decryption key, said key-synchronizing destination node comprising: means for receiving and storing one or more new decryption keys from a source node from which encrypted packets are being transmitted; means for monitoring received data packets for any packet having a predetermined format; and means for activating a new decryption key upon detection of a received packet having the predetermined format.

Preferably, said predetermined format includes a predetermined binary value inserted into one or more predetermined bit positions in the header portion of each data packet to be decrypted using the new decryption key.

Preferably, said data packet having a predetermined format is a marker cell.

Preferably, the predetermined binary value comprises the binary complement of the bit value stored in the corresponding predetermined bit positions of the header portion of the prior data packet.

Brief Description of the Drawings

While the specification concludes with claims particularly pointing out and distinctly claiming that which is regarded as the present invention, details of the invention may be more readily ascertained from the following detailed description when read in conjunction with the accompanying drawings wherein:

Figure 1 is a simplified view of major components of a conventional network in which the present invention may be practised;

Figure 2 shows the high level format of a conventional standard Asynchronous Transfer Mode (ATM) cell;

Figure 3 is a simplified view of the major functional components of a source node capable of implementing the present invention;

Figure 4 is a simplified view of the major functional components of a destination node capable of implementing the present invention;

Figure 5 depicts an ATM cell with a format modification according to a first embodiment of the present invention;

Figure 6 is a flow chart of operations that are performed at a source node when use of a new encryption key is to be initiated;

Figure 7 is a flow chart of operations that are performed at a destination node in order to maintain synchronization between the keys used to encrypt a particular data packet at a source node and to decrypt the same data packet upon its receipt at a destination node;

Figure 8 is a flow chart of key synchronization operations that are performed at source node in accordance with the present invention;

Figure 9 shows the format of a marker packet which can be used in key synchronization operations in a second embodiment of the present invention;

Figure 10 is a flow chart of key synchronization operations that are performed at a destination node when the marker packet of Figure 9 is received;

Figure 11 shows an alternate form of marker packet defined using existing fields in a standard ATM cell in accordance with a third embodiment of the present invention; and

Figure 12 is a flow chart of key synchronization operations that are performed at a destination node when the marker packet of Figure 11 is employed.

Description of Preferred Embodiments

In the following description, the terms "cell" and "packet" may be used interchangeably to refer to a data unit consisting of a header portion and a data payload portion. For purposes of interpreting the description and the claims, it should not be assumed that the term "cell" is limited to a fixed length data unit or that the term "packet" is limited to a variable length data unit.

In any data communication network, the ultimate objective is to be able to transport data from a first user

to a second user. While the term "user" is typically assumed to mean a human user, from a network standpoint, the actual data users are devices such as processors, printers or even workstations, such as the workstations 10 and 18 shown in Figure 1. The workstations 10 and 18 are connected to a shared wide area network 14 through intermediate communication processors 12 and 16, respectively. The functions performed by communication processors vary depending upon the characteristics of the wide area network and of the attached workstations. For example, if the wide area network 14 implements Asynchronous Transfer Mode (ATM) protocols, a communication processor might handle the functions of segmenting data received from a workstation into a series of fixed length data cells and of generating a header for each cell with information needed to transfer the cell through the network. Such functions are generally referred to as ATM adaption functions. The same processor might be used to encrypt that data. A counterpart processor at the receiver would reassemble the data into a format usable by the receiving workstation by decrypting the data contained in received cells and by reassembling the data into longer data segments usable by the receiving workstation.

Referring to Figure 2 and as noted earlier, a standard ATM cell includes a five byte header field 20 which contains control and routing information for the cell and a forty-eight byte data field 22 which contains the actual user data and possibly an error checking character. From time to time, the data field 22 may be referred to as the "data payload" or just the "payload" of the cell. While use of an embodiment of the invention, as described below, causes the contents of the header field to be altered, the same basic five byte header and forty-eight byte data structure is maintained at all times within the network.

For data to be successfully transferred in encrypted form from a source, such as workstation 10, to a destination, such as workstation 18, the devices which actually perform the encryption/decryption operations must synchronise their use of encryption/decryption keys. The necessary functions may be implemented either in software executed by a general purpose processor or as firmware or microcode written for a special purpose processor. In either case, some hardware, such as buffer registers or memory is employed in the course of the process. Figure 3 is a block diagram of functional components required to implement the invention at a source node 24. The source node 24 necessarily includes a processor or CPU 26 which operates under the control of an operating system 28 as well as memory components 30 for storing both data and program instructions. Assuming data supplied to the source node 24 is not already in standard ATM cell format, the system may include an ATM adapter component 36, which will convert received data to standard ATM format. The source node 24 also includes an encryption controller 32 which performs required encryption operations on

the data payload of each ATM cell and a key synchronization system 34. The key synchronization system 34 will store needed encryption keys and perform other operations, to be described in more detail below, required to assure synchronisation of encryption and decryption keys in active use at source and destination systems. The source node will further include a packet transmission component 38 for transmitting ATM cells after the data payloads in the cells are encrypted using the current encryption key.

Referring to Figure 4, a destination node 40 will have a number of components which also exist in a source node. For example, any destination node capable of implementing the present invention will include a CPU 42, an operating system 44 and memory 46. In fact, a given node ordinarily can operate either as a source system or a destination system at different times, which means that the same processor or operating system or memory will perform source or destination functions at different times. A destination node will also include a packet receiving system 48 for receiving ATM cells from the wide area network, a decryption controller 50 for decrypting the data payload of each cell and a key synchronization system 54 for making sure that the decryption key used for a particular ATM cell corresponds to the encryption key used in encrypting that same cell. Finally, unless the data is to be transported from the destination node in native ATM cell format, the node will include an ATM adapter function 52 for performing any necessary cell sequencing and desegmentation operations.

In a first embodiment of the invention and as shown in Figure 5 of the drawings a single bit position in one of the five header bytes of a standard ATM cell is defined as a key synchronization bit (KSB) position 56. A change in the binary value stored in KSB position 56 from one data packet to the next is a signal to a destination node that a new decryption key (previously sent to and stored by the node) is to be activated. Once the new decryption key is activated, the KSB value in packets received at the node should remain constant until another new decryption key is to be activated.

Figure 6 is a flow chart of steps that are performed at a source node in maintaining key synchronization in accordance with a preferred embodiment of the invention. It is assumed that the source node is already sending data packets as part of a process which is asynchronous to the key synchronization process being described. The point of entry into the key synchronization process is a test 60 whether the current encryption/decryption keys are to be updated (changed). If the keys are to be updated, the new decryption key is sent to the destination node in an operation 62, using a conventional secure and reliable key exchange protocol. The specific key exchange protocol employed is not critical to the present invention. It only matters that the new key is sent to the destination node at which it is eventually to be used.

Even after the key is sent, data packets will con-

tinue to be encrypted using the old key until a decision is made to activate the new key. In theory, a test 64 could be applied to a key just sent to the destination node or to a key sent at some earlier point in time. In either case, if test 64 shows the new key is to remain idle, data packets will continue to be encrypted and transmitted (operation 68) with the current KSB value. As a specific example, if the KSB value had been set to a "1" when the current encryption key was first used, it will remain at "1" for each data packet encrypted using the current key.

However, when the new key is activated, the KSB value will be set to "0" in any data packet encrypted and sent (operation 66) using the new key. Each time a new key is activated, the KSB value will be toggled to the complement of its former binary value.

Figure 7 is a flow chart of operations that are performed at a destination node. Such a node receives and stores (operation 70) a new decryption key. The destination node continues to receive data packets (operation 72). When each packet is received, the binary value stored in the KSB position in its header is read (operation 74) and tested (operation 76) against the KSB value found in the preceding data packet. If the KSB value has not changed, the destination node continues to use the current decryption key (operation 78) to decrypt the packet. If, however, the KSB value has changed, the new key is retrieved from storage and activated to decrypt the packet payload in an operation 80.

While a single KSB bit position is employed in this first embodiment, multiple bit positions could be assigned to the cell header.

Key synchronization operations can also be performed using special purpose cells, called marker cells, to notify a destination node that it is to activate a previously received decryption key. Figure 8 is a flow chart of steps that are performed at a source node in maintaining key synchronization using either of two types of marker cells, both of which will be described in detail later. It is assumed that the source node sends data packets as part of a packet send process 60. Symbol 62 is intended to represent that the packet send process 60 operates in parallel with and asynchronously to the key synchronization process. The point of entry into the key synchronization process is a test 64 whether a key update is to occur; that is, whether a new decryption key is to be sent to a destination node to which data packets are currently being transmitted. If a key update is to occur, the new decryption key is sent to the destination node in an operation 66 using a conventional secure and reliable key exchange protocol. The specific key exchange protocol employed is not critical to the present invention. It only matters that the new key is sent to the destination node at which it is eventually to be used.

After the new key is sent, the source node continues to use the old encryption key (operation 68) to encrypt data packets until a test 70 shows that the new decryption key is to be activated at the destination node.

Once a decision is made to activate the new decryption key, key synchronization is initiated by having the source node transmit a marker packet (operation 72) to the destination node. The unique format of a marker packet is used to distinguish it from a data packet. The marker packet is encrypted using the old encryption key.

Upon transmission of the marker packet, the source node starts a marker acknowledgment timer (operation 74) and begins encrypting data packets using the new encryption key (operation 76) and sending those data packets to the destination node. The source node then begins to listen for an acknowledgment from the destination node that the marker packet has been received. If the acknowledgment is received while the marker acknowledgment timer is still running, the timer is reset and the normal packet send process 60 continues. If, however, no acknowledgment has been received, a test 80 is conducted to determine the marker acknowledgment timer has expired. If the timer has expired, another marker packet is transmitted and the timer is restarted. If the timer has not yet expired, the normal packet send process 60 continues with data packets being encrypted using the new encryption key.

Figure 9 shows the format of one type of suitable marker packet according to a second embodiment of the present invention. It is assumed that the packet again has the general form of a standard ATM cell with a five byte header field 82 and a forty-eight byte data field or payload 84. For this type of marker packet, the ATM header field 82 remains unchanged, but payload 84 includes several nonstandard fields; namely a current key field 86, a new key field 88 and a random seed field 90. The value stored in field 86 defines the key currently in use at the destination node. The value stored in field 88 defines the new key, already sent to and stored at the destination node. The random seed field is simply a random number which is used to pad the bit positions that would otherwise remain empty between the new key field 88 and a CRC field 92 used to store an error checking character.

Once the current key, the new key and the random seed have been written into the first "n" positions of the data field 84, the value of an error checking character is calculated based on the data in these positions. The specific process used to calculate the error checking character is not significant to the present invention. Preferably, a standard CRC (Cyclical Redundancy Check) process is used. The calculated CRC character is written into the CRC bit positions and the entire data field 84 is then encrypted using the current encryption key.

Figure 10 is a flow chart of operations that are performed at a destination node at which decryption operations must be synchronized with encryption operations being performed as a connected source node. The destination node receives and stores a new decryption key in an operation 94 which is asynchronous to a normal packet receiving process 96. The data field of each packet received at the destination node is decrypted in

an operation 98 using the currently active decryption key. The decryption operation restores the original data to the packet data field.

The identification of valid marker packets begins with the extraction (operation 100) of the values stored in the current key bit positions, the new key bit positions and the CRC bit positions in a packet's decrypted payload. A CRC value is then calculated at the destination node (operation 102) based on the data in the first "n" bit positions in the data field and compared (operation 104) to the extracted CRC value. If the calculated and extracted values are not equal, it is assumed that the packet is not a marker packet. The packet is forwarded in the destination node system for further processing in an operation 108.

If, however, the calculated and extracted CRC values match, which tentatively identifies the received packet as a marker packet, the identification is tested further in an operation 106 which compares the extracted current and new key values to the current and new key values, respectively, already stored at the destination node. If the keys' values fail to match, the packet is not considered to be a valid marker packet. If the keys' values do match, the packet is treated as a marker packet.

A marker packet acknowledgment is returned to the source node in an operation 110. The marker packet itself is discarded in an operation 112 and the destination node activates the new decryption key and applies it to subsequently received packets. The normal packet reception process then continues until the next key update operation.

The process described with reference to Figures 9 and 10 requires the generation of a marker packet having a special non-standard format. According to a third embodiment of the invention, a standard ATM cell can be used as a marker cell by extending the existing definitions of certain cell field values. Referring first to Figure 11, a standard ATM cell header includes a three bit Payload Type subfield which identifies the type of data payload in the cell. Bit 0 of the subfield is set to "0" for a cell containing user data and to "1" for a cell carrying network operations and administration (OAM) or traffic control and resource management (RM) data. For simplicity, OAM and RM cells are referred to generically as management cells.

Each management cell contains, within the payload, a second field that more precisely identifies the function of the cell. While a number of cell functions have already been defined by ATM standards, a new function definition can be added; namely, a definition of a ATM management cell as a marker cell for purposes of key synchronization.

Figure 12 is a flow chart of steps that are performed at a destination node in maintaining key synchronization where marker packets having the Figure 11 format are employed. As before, a process 120 for receiving new decryption keys and for storing those keys operates asynchronously and in parallel with a normal packet

receiving process 122. The payload of each received packet is decrypted (operation 124) using the decryption key currently active at the destination node.

A check 126 is then made to determine whether a new key has been received and stored without a new marker cell having subsequently been found. The purpose of check 126 is to reduce the number of packets which must be examined to determine whether they are marker packets. The only condition under which a marker cell should logically exist is where a new key has been received but not a marker cell activating that key. Under other conditions, indicated by a "no" response to test 126, the cell is assumed to be something other than a marker cell and is forwarded (operation 140) by the destination node for further processing.

In one embodiment of the invention, the number of potential marker cells which must be analyzed following test 126 can be reduced by making use of existing ATM standard definitions for the Payload Type field in a cell header. According to current ATM standards, Bit 2 of the Payload Type field is set to "1" to indicate the end of a data block and to "0" to indicate the beginning or middle of a data block. If Bit 2 of the Payload Type field in a marker cell is always set to "1", a test 128 of the Bit 2 value can be used to eliminate from marker cell analysis any cell in which Bit 2 = "0".

If test 128 fails to rule out a particular cell, then another test 130 is used to determine whether the cell is an ATM management cell. As noted earlier, management cells are defined by setting Bit 0 of the cell's Payload Type field = "1". If test 130 finds Bit 0 = "1", the cell is tentatively identified at least as a management cell. To determine whether this management cell is really a marker cell, the cell definition field in the payload is tested (operation 132) to see if that field contains the appropriate marker cell definition.

Any cell which fails to satisfy any of tests 126, 128, 130 and 132 is assumed not to be a marker cell and is forwarded by the destination node. Certain of the listed tests are useful but not essential to a determination whether a particular cell is a marker cell. Specifically, the actual analysis whether a particular cell is a marker cell can be done relying on tests 130 and 132 alone. Tests 126 and 128 are not essential to that analysis but are likely to improve performance of the system by reducing the number of cells which must be analyzed using tests 130 and 132.

Once the destination node finally identifies a particular cell as being a marker cell, a marker acknowledgment message is returned to the source node in an operation 134. The marker cell is discarded in an operation 136 and subsequently received cells are decrypted (operation 138) using the new decryption key. Decryption using the new key continues until a replacement key is provided to the destination node in a subsequent key update operation.

While preferred embodiments of the invention are described, variations and modifications will occur to those skilled in the art once they become aware of the

basic inventive concepts. For example, while the preferred embodiment calls for new keys to be distributed from a source node one at a time, it is within the scope of the present invention to distribute several keys to a destination node during a single key update operation. The destination node could store the keys in a list and could activate the next key on the list each time a new marker cell is detected. Finally, while the invention has been described for use in an ATM environment with its fixed length cells, it could also be effectively employed in systems in which variable length packets are used.

It is intended that the appended claims shall be construed as covering the preferred embodiment and all variations and modifications, including those described above, that fall within the true spirit and scope of the invention.

Claims

1. For use in a system including one or more source nodes for encrypting data using an encryption key, an interposed data communication network through which packets including the encrypted data can be transmitted, each of said packets including a header and a data payload, and one or more destination nodes capable of decrypting received data using a decryption key, a method of maintaining synchronization between the encryption key used at a source node to encrypt data and the decryption key used at the destination node to decrypt data, said method comprising the steps of:

sending a new decryption key from the source node to the destination node;

storing the new decryption key at the destination node;

at the source node, transmitting a data packet having a predetermined format when the new decryption key is to be activated;

at the destination node, monitoring each received data packet to determine whether the packet has the predetermined format; and

at the destination node, when a packet having the predetermined format is detected, activating the new decryption key for use in decrypting subsequently received packets.

2. For use in a system including one or more source nodes for encrypting data using an encryption key, an interposed data communication network through which data packets including the encrypted data can be transmitted, each of said data packets including a header portion and a data payload portion, and one or more destination nodes for decrypting received data packets using a decryption key, a

key-synchronizing system for maintaining synchronization between the encryption key used at a source node to encrypt data and the decryption key used at the destination node to decrypt data, said key-synchronizing system comprising:

5

at a source node from which the encrypted packet is to be sent, means for sending at least one new decryption key to the destination node which is to receive the packet;

10

at the destination node, means storing each new decryption key that is received;

at the source node, means for generating a data packet having a predetermined format;

15

at the destination node, means for monitoring each received data packet and for determining whether the packet has the predetermined format; and

20

at the destination node, means responsive to the identification of a received data packet having the predetermined format for retrieving a new decryption key from storage and for initiating use of that key to decrypt each subsequently received data packet.

25

3. A key-synchronizing source node for use in a system including one or more source nodes for encrypting data using an encryption key, an interposed data communication network through which data packets including the encrypted data are transmitted, each of said data packets including a header portion and a data payload portion, and one or more destination nodes for decrypting received data packets using a decryption key, said key-synchronizing source node comprising:

30

35

means for sending at least one new decryption key to a destination node to which data packets are to be sent;

40

means for generating a data packet having a predetermined format, indicating that a new decryption key is to be activated at a destination node to which the data packet having the predetermined format is sent; and

45

means for sending the data packet having the predetermined format to at least one destination node.

50

4. A key-synchronizing destination node for use in a system including one or more source nodes for encrypting data using an encryption key, an interposed data communication network through which data packets including the encrypted data is trans-

55

mitted, each of said data packets including a header portion and a data payload portion, and one or more destination nodes for decrypting received data packets using a decryption key, said key-synchronizing destination node comprising:

means for receiving and storing one or more new decryption keys from a source node from which encrypted packets are being transmitted;

means for monitoring received data packets for any packet having a predetermined format; and

means for activating a new decryption key upon detection of a received packet having the predetermined format.

5. The invention of any preceding claim wherein said predetermined format includes a predetermined binary value inserted into one or more predetermined bit positions in the header portion of each data packet to be decrypted using the new decryption key.

6. The invention of any of claims 1 to 4, wherein said data packet having a predetermined format is a marker cell.

7. The invention of claim 5 further wherein the predetermined binary value comprises the binary complement of the bit value stored in the corresponding predetermined bit positions of the header portion of the prior data packet.

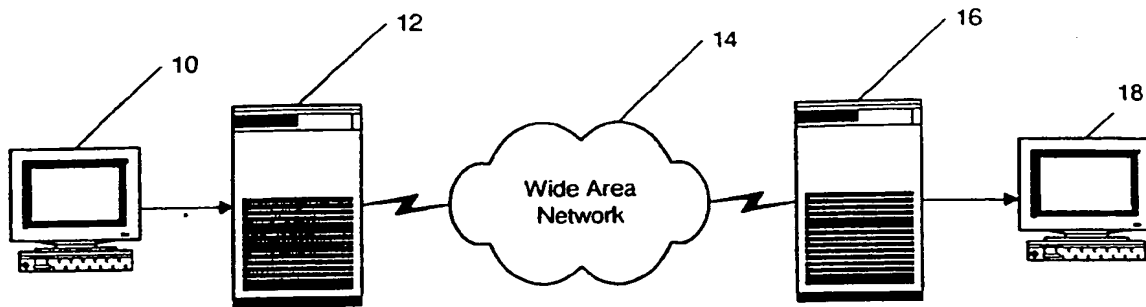


Fig. 1
(Prior Art)

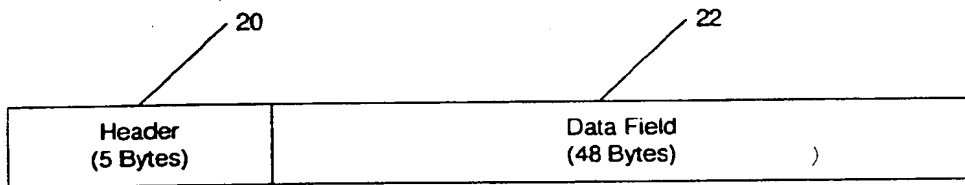


Fig. 2
(Prior Art)

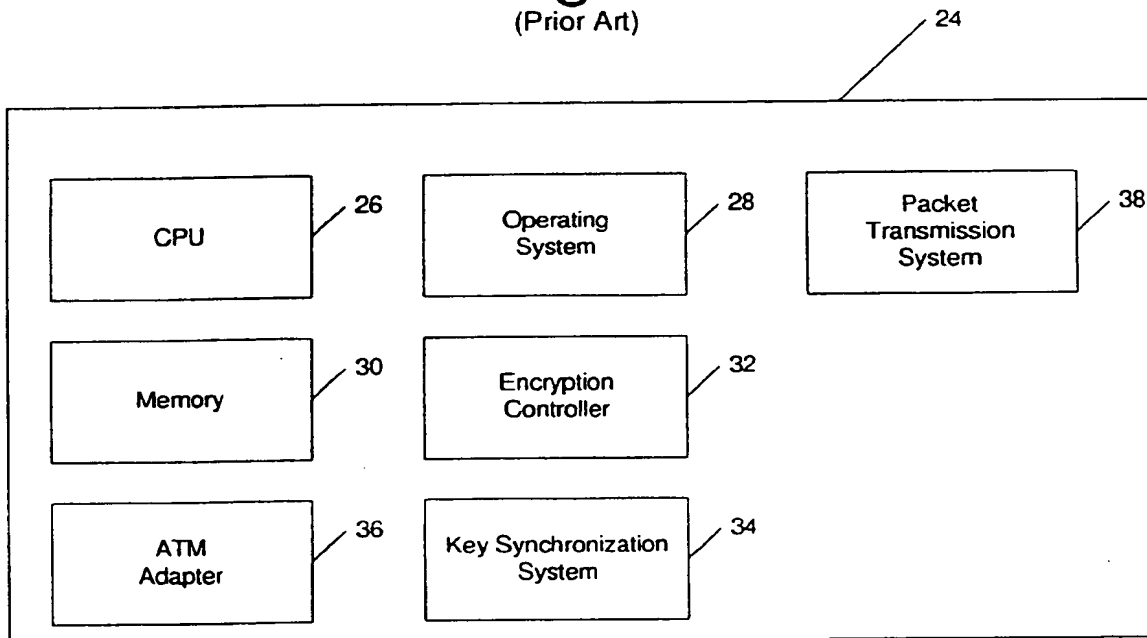


Fig. 3

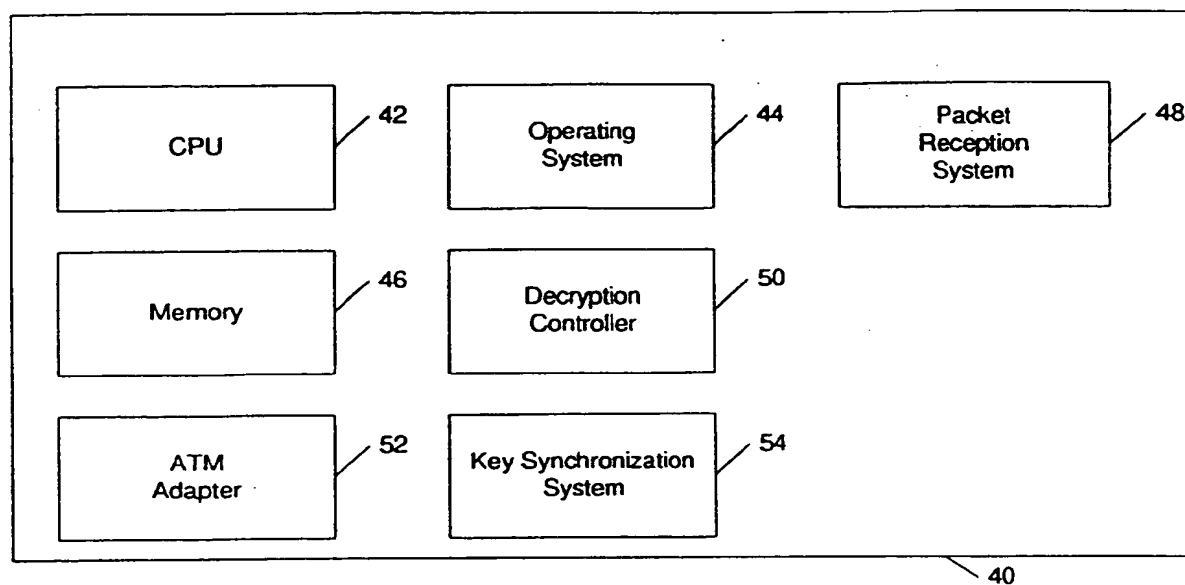


Fig. 4

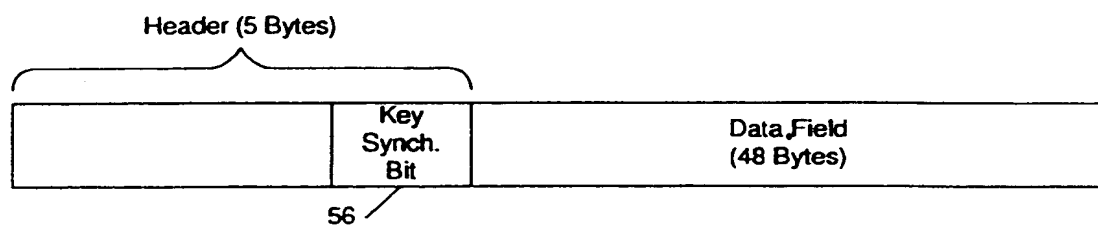


Fig. 5

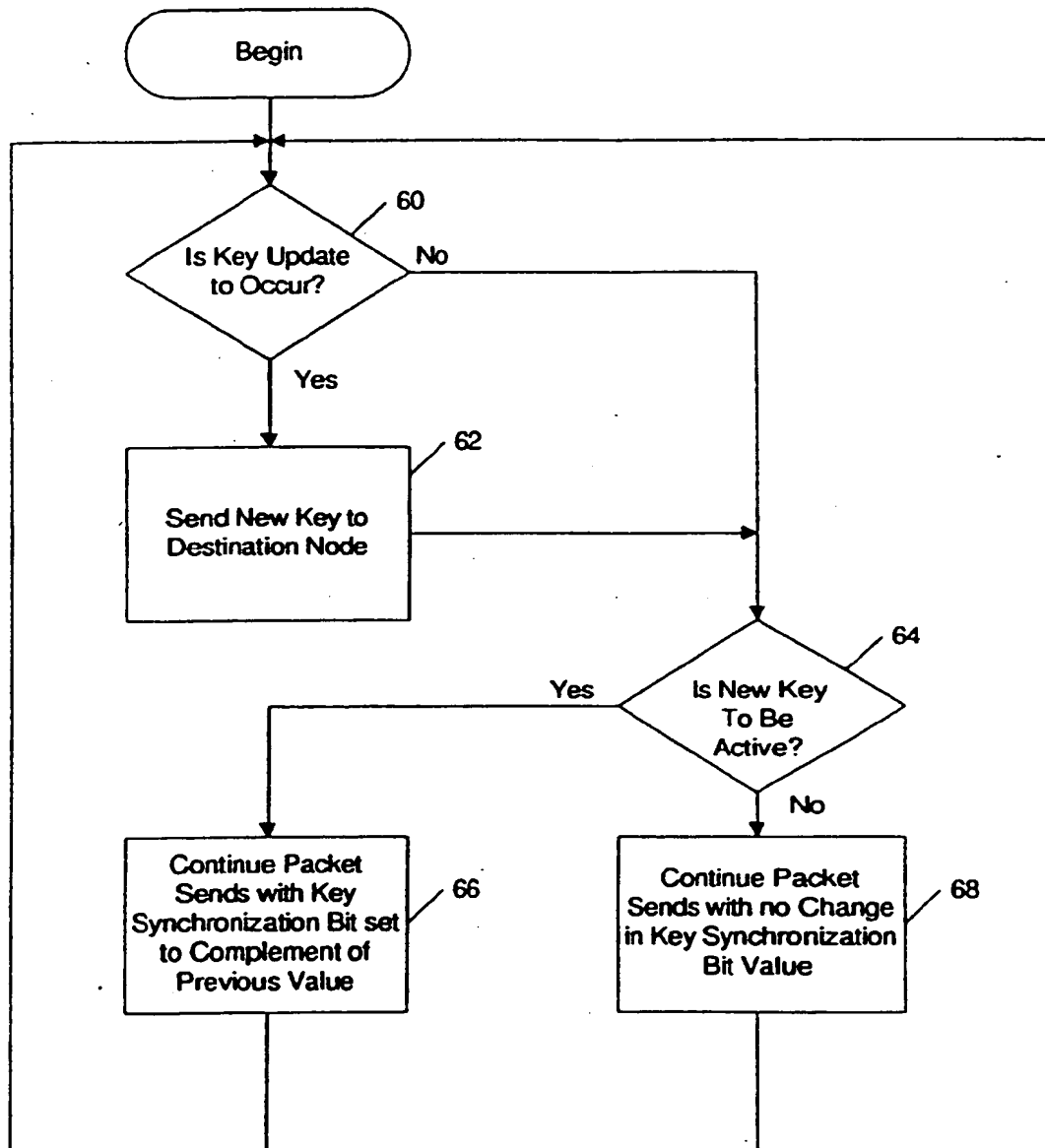
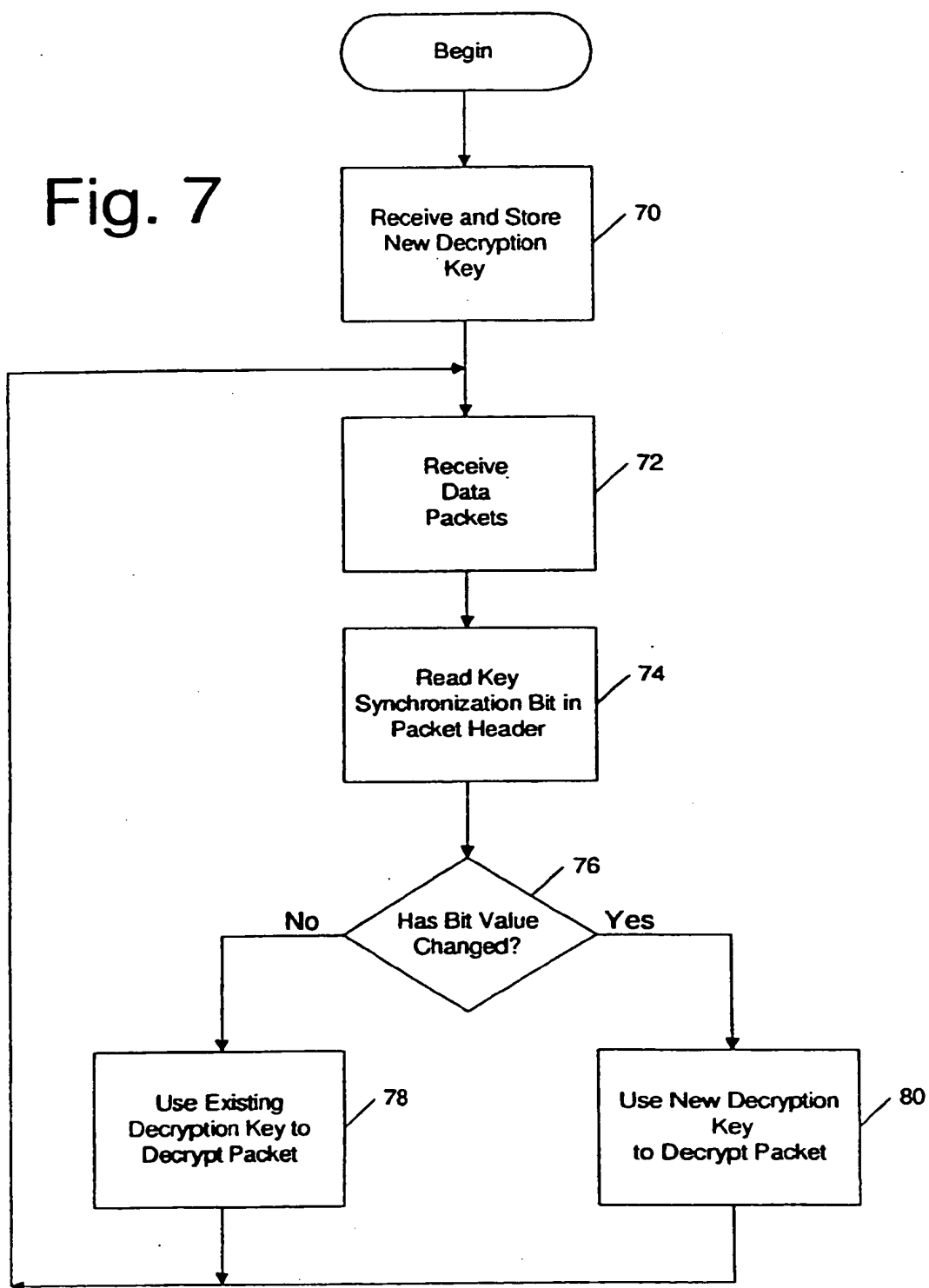


Fig. 6

Fig. 7



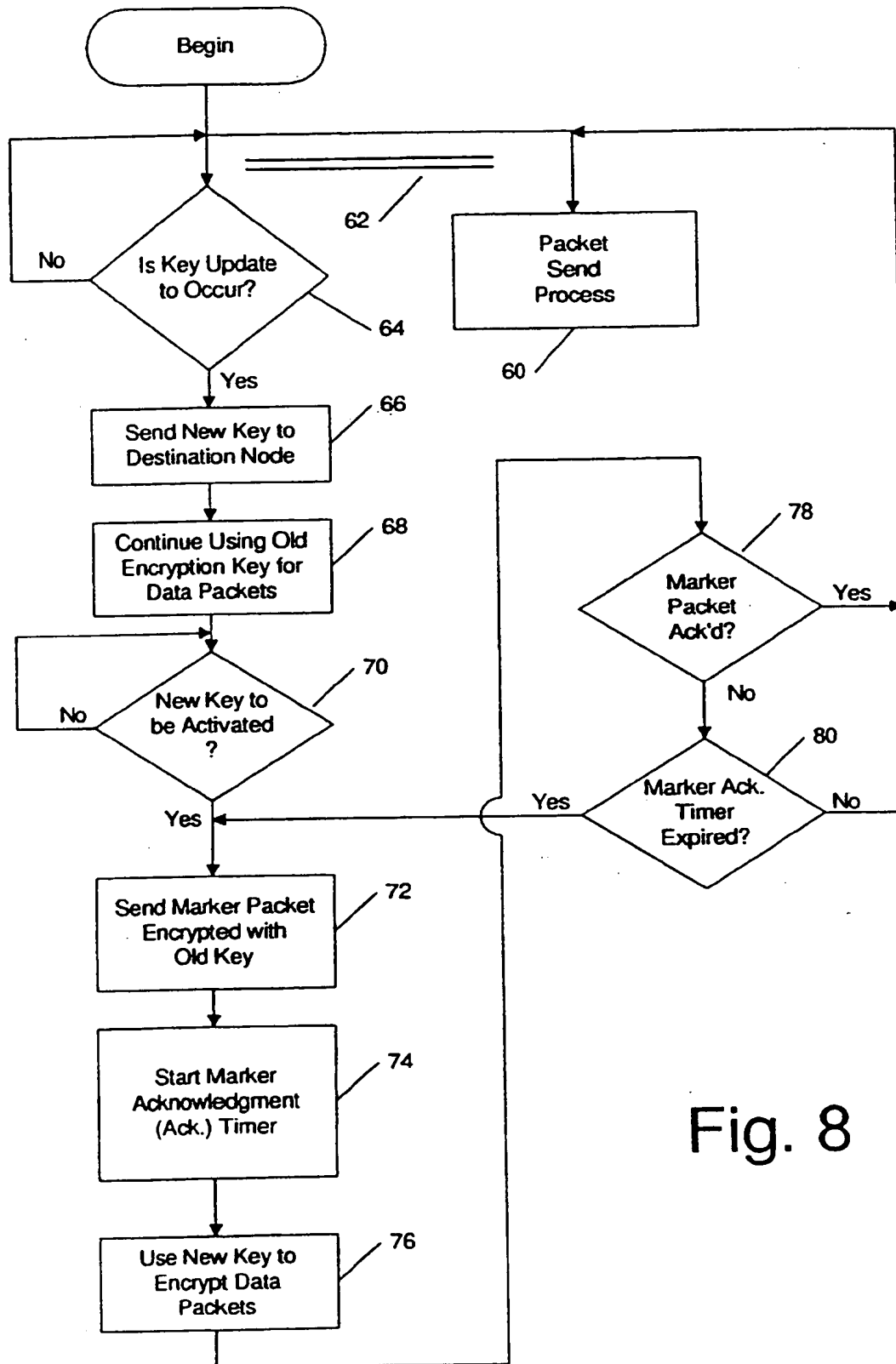


Fig. 8

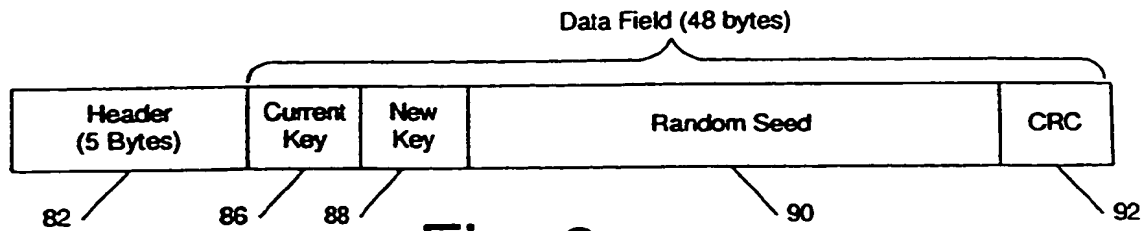


Fig. 9

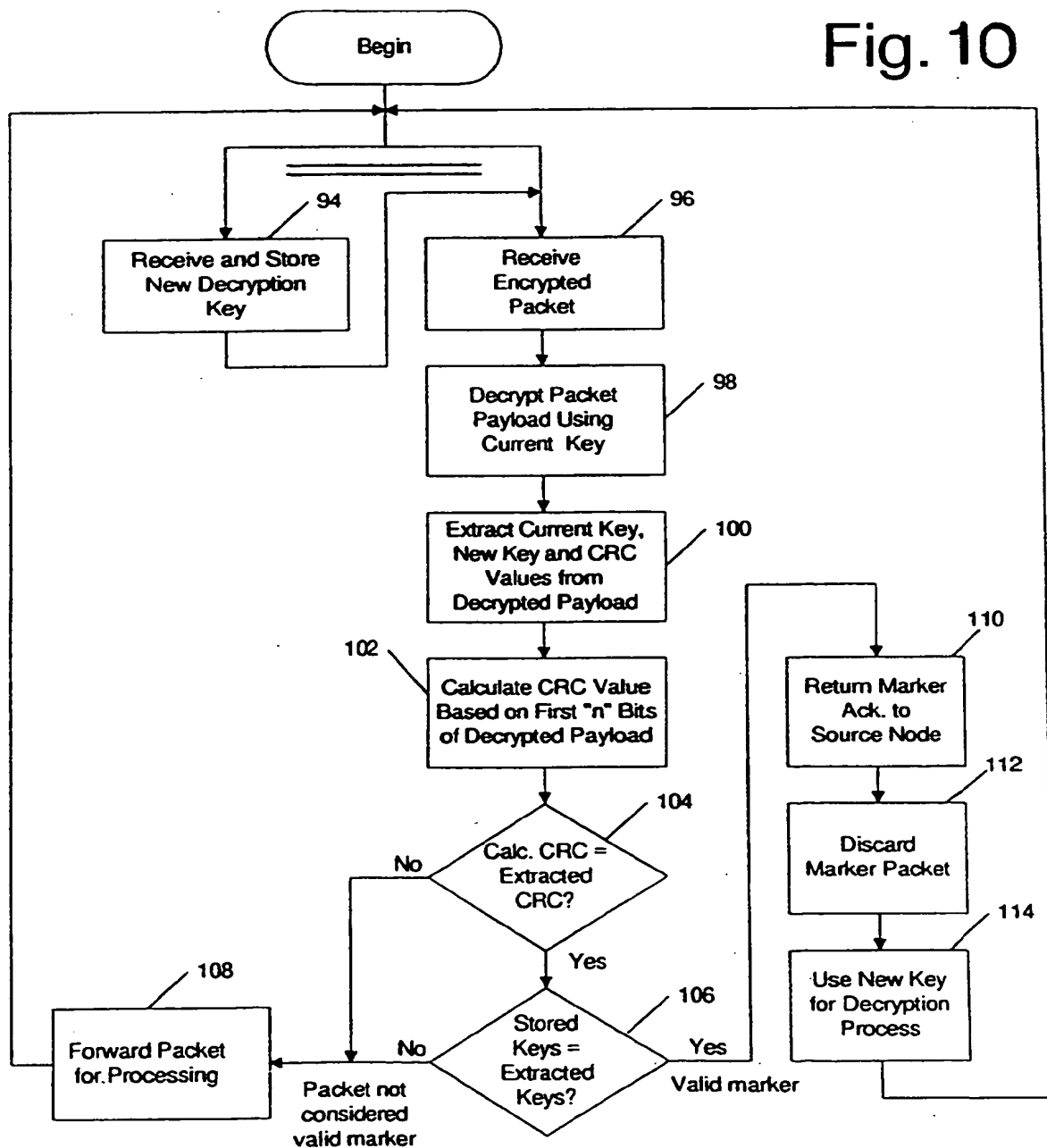


Fig. 10

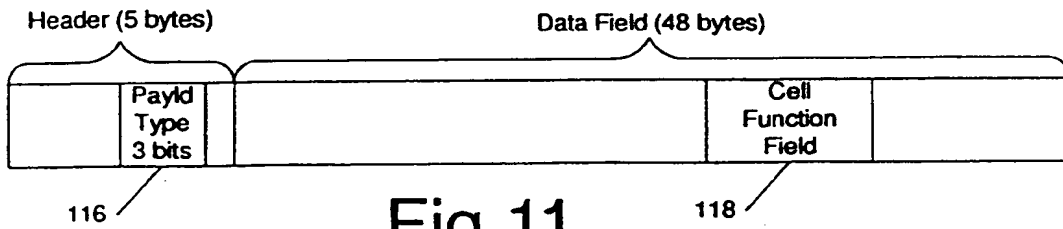


Fig. 11

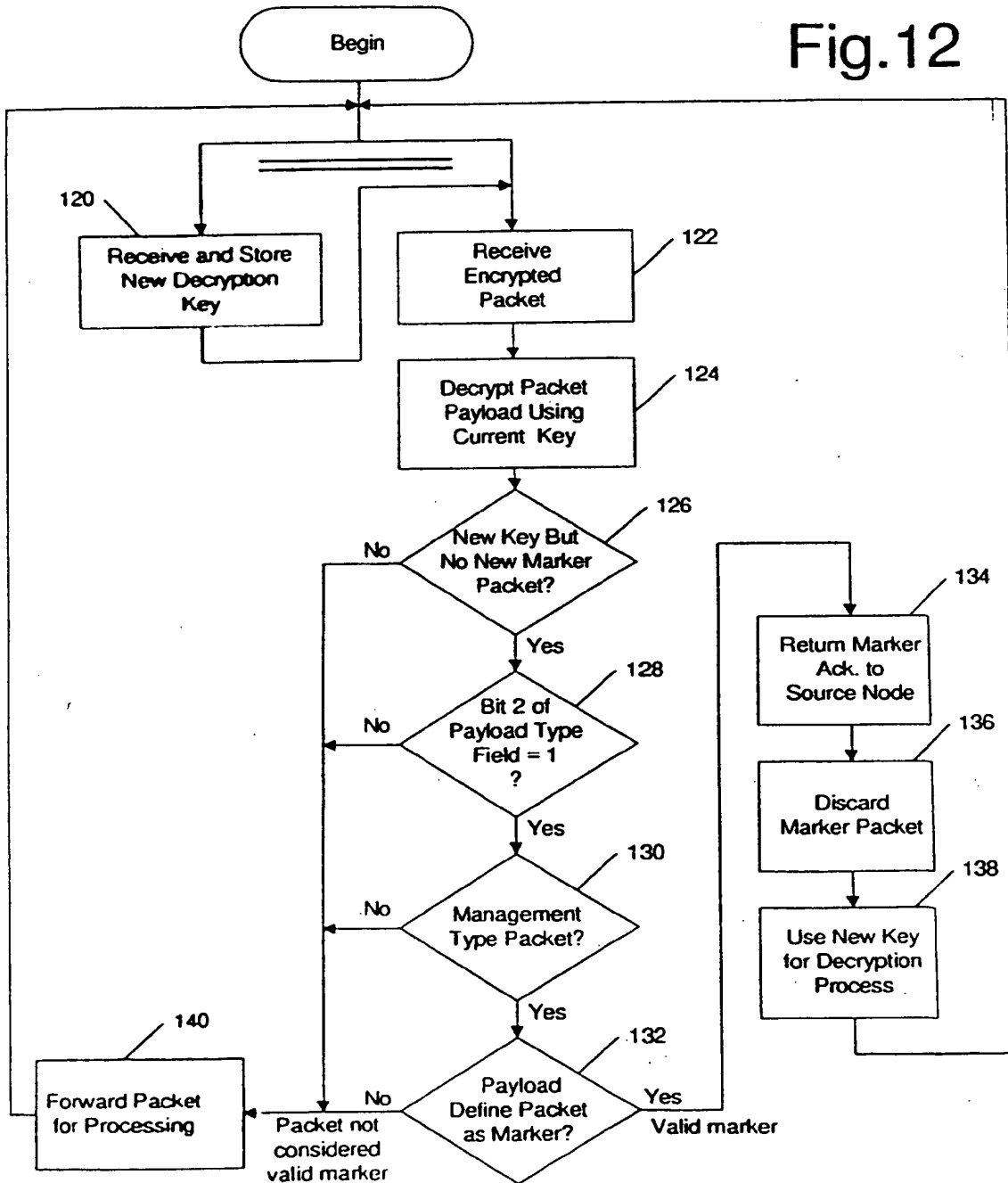


Fig. 12



(19)

Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 0 786 881 A3

(12)

EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
01.03.2000 Bulletin 2000/09

(51) Int. Cl.⁷: H04L 9/12

(43) Date of publication A2:
30.07.1997 Bulletin 1997/31

(21) Application number: 96309516.1

(22) Date of filing: 27.12.1996

(84) Designated Contracting States:
DE FR GB

(30) Priority: 29.01.1996 US 592931
29.01.1996 US 592903

(71) Applicant:
INTERNATIONAL BUSINESS MACHINES
CORPORATION
Armonk, NY 10504 (US)

(72) Inventors:
• Gray, James P.
Chapel Hill, NC 27514 (US)

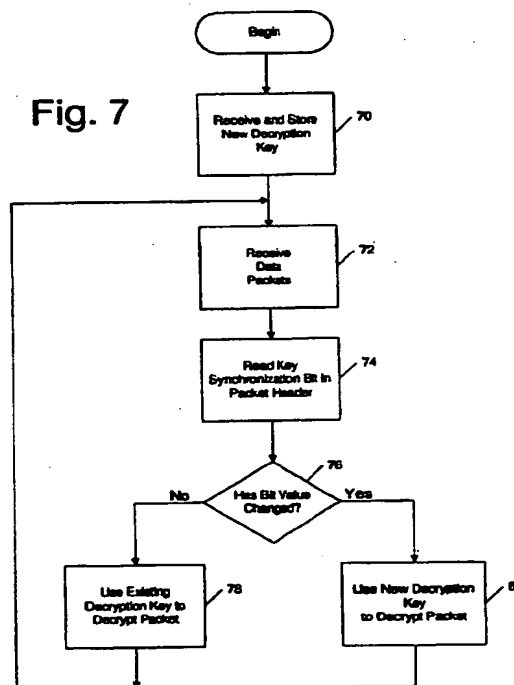
• Onvural, Raif O.
Cary, NC 27513 (US)
• Peyravian, Mohammed
Cary, NC 27513 (US)

(74) Representative:
Moss, Robert Douglas et al
IBM United Kingdom Limited
Intellectual Property Department
Hursley Park
Winchester Hampshire SO21 2JN (GB)

(54) Method and system for synchronisation of encryption/decryption keys in a data communications network using marker packets

(57) To enhance the security provided by data encryption in a data communication network, encryption/decryption keys are changed periodically at the source and destination nodes for an established connection. A destination node must know not only the value of any new key but also when to begin using that key to decrypt received data packets. Synchronization (making sure a data packet is decrypted using a decryption key correlated with the encryption key used to encrypt the same packet) is achieved through the use of marker cells, special purpose cells. When a source node decides to activate a new key, previously sent to and stored at the destination node, a marker cell is transmitted by the source node to the destination node. When the destination node recognizes the marker packet, it discards it and activates the previously received key for use in decrypting subsequently received packets.

Fig. 7





European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 96 30 9516

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	DE 34 18 571 A (GRETAG AG) 22 November 1984 (1984-11-22) * page 7, paragraph 2; claim 1 *	1-7	H04L9/12
X	STEVENSON D ET AL: "Secure communications in ATM networks" COMMUNICATIONS OF THE ACM, FEB. 1995, USA, vol. 38, no. 2, pages 45-52, XP000505359 ISSN: 0001-0782 * page 47, column 2 - page 48, column 1 * * page 48, column 3 - page 49, column 1 *	1-7	
P, X	SHAW-CHENG CHUANG: "Securing ATM networks" 3RD ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, PROCEEDINGS OF 3RD ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY, NEW DELHI, INDIA, 14-16 MARCH 1996, pages 19-30, XP000620974 1996, New York, NY, USA, ACM, USA ISBN: 0-89791-829-0 * page 25, column 1 *	1-7	
X	US 4 965 804 A (TRBOVICH NICK G. ET AL) 23 October 1990 (1990-10-23) * abstract *	1-7	
A	EP 0 667 691 A (ELEMENTRIX TECHNOLOGIES LTD) 16 August 1995 (1995-08-16) * page 7, line 23 - page 8, line 27 *	1-5	TECHNICAL FIELDS SEARCHED (Int.Cl.6) H04L
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 5 January 2000	Examiner Zucka, G
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document			

EPO FORM 1503 03/82 (P04C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 96 30 9516

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

05-01-2000

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
DE 3418571	A	22-11-1984	CH	658759 A	28-11-1986
US 4965804	A	23-10-1990	US	5048087 A	10-09-1991
EP 0667691	A	16-08-1995	IL	108645 A	30-09-1997
			AU	1158095 A	24-08-1995
			CA	2141882 A	15-08-1995
			CN	1117227 A	21-02-1996
			JP	7288521 A	31-10-1995
			US	5703948 A	30-12-1997

EPO FORM P459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

THIS PAGE BLANK (USPTO)